Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for performing authentication of messages in a dual processor device, wherein the dual processor device receives encrypted messages and wherein the dual processor device includes a host processor coupled to a secure processor, the method comprising:

receiving an encrypted message at the dual processor device;

using the secure processor of the dual processor device to decrypt the message;

using the secure processor of the dual processor device to authenticate the message via an authentication calculation so as to determine whether the message is authentic; and then

if said message is authentic, transferring the decrypted message to the host processor for use by the host processor**, and if the message is not authentic, not transferring the decrypted message to the host processor**.

2. (Previously presented) The method as claimed in claim 1 wherein said receiving the encrypted message comprises:

receiving the encrypted message at a cable telephony adapter.

3. (Previously presented) The method as claimed in claim 1 wherein said dual processor device is a cable telephony adapter, said method further comprising:

coupling said cable telephony adapter with a telephony network;

coupling said cable telephony adapter with a gateway controller;

coupling said cable telephony adapter with a user computer.

4. Previously presented) The method as claimed in claim 3 and further comprising:

coupling a second cable telephony adapter with said telephony network;

coupling a second gateway controller with said second cable telephony adapter;

coupling a second user computer with said second cable telephony adapter.

5. (Previously presented) The method as claimed in claim 4 and further comprising:

establishing a communication between said user computer and said second user computer via said cable telephony adapter and said second cable telephony adapter.

6. (Previously presented) The method as claimed in claim 4 and further comprising:

coupling a provisioning server with said cable telephony network.

7. (Previously presented) The method as claimed in claim 4 and further comprising:

coupling a billing host with said cable telephony network.

8. (Previously presented) The method as claimed in claim 4 and further comprising:

coupling a customer service representative center with said cable telephony network.

9. (Previously presented) The method as claimed in claim 4 and further comprising:

transmitting clear text to the user computer.

10. (Previously presented) The method as claimed in claim 9 and further comprising:

receiving clear text from the user computer.

11. (Previously presented) The method as claimed in claim 1 and further comprising:

receiving an authentication certificate for said encrypted message; and

wherein said using the secure processor to authenticate the message comprises using the certificate to authenticate the message.

12. (Previously presented) The method as claimed in claim 1 and further comprising:

using the authentication certificate to confirm the legitimacy of a public key.

13. (Previously presented) The method as claimed in claim 1 wherein said using the secure processor to authenticate the message comprises:

utilizing a public key to verify a signature.

14. (Previously presented) The method as claimed in claim 1 and further comprising:

storing decryption and authentication keys on the secure processor.

15. (Currently amended) An apparatus for use in a telephony system, said apparatus comprising:

an input for receiving an encrypted message;

a host processor for processing unencrypted data;

a secure processor coupled with said host processor in said apparatus, wherein said secure processor is configured to decrypt said encrypted message and authenticate said encrypted message utilizing an authentication certificate**, to permit transfer of the decrypted message to said host processor if the message is authentic, and to not permit transfer of the decrypted message if the message is not authentic**.

16. (Previously presented) The apparatus as described in claim 15 wherein said secure processor is further configured to transfer said decrypted message to said host processor after decrypting said encrypted message.

17. (Previously presented) The apparatus as described in claim 15 wherein said input for receiving said encrypted message comprises an input for receiving said encrypted message from a telephony network.

18. (Previously presented) The apparatus as described in claim 15 and further comprising:

an output for outputting clear text to a user computer.

19. (Previously presented) The apparatus as described in claim 18 and further comprising:

an input for inputting clear text from the user computer.

20. (Previously presented) The apparatus as described in claim 15 wherein the apparatus is coupled with a gateway controller.

21. (Previously presented) The method as claimed in claim 4 and further comprising:

storing certificates in memory in said dual processor device.

22. (New) A method for providing secure processing in a telecommunication system having a dual processor device, wherein the dual processor device receives encrypted messages and wherein the dual processor device includes a host processor that uses unencrypted data and that is coupled to a secure processor, the method comprising:

receiving an encrypted message at the secure processor;

using the secure processor to decrypt the message;

using the secure processor to determine whether the message is authentic; and then

transferring the decrypted message from the secure processor to the host processor for use by the host processor, only if the message is determined to be authentic by the secure processor.